67 -/0 - 6D

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s):

       Louis H. Sciupac

WARNING: Patent must be applied for in the name(s) of all of the actual inventor(s). 37 CFR 1.41(a) and 1.53(b).

For (title):

SECURE TRANSACTIONS WITH PASSIVE STORAGE MEDIA

CERTIFICATION UNDER 37 C.F.R. 1.10*
(Express Mail label number is mandatory.)
(Express Mail certification is optional.)

I hereby certify that this New Application Transmittal and the documents referred to as attached therein are being deposited with the United States Postal Service on this date ___July 6, 2000___ in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL471851545US , addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

                          ___Sally Azevedo___
                      (type or print name of person mailing paper)

                        Signature of person mailing paper

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

WARNING: Each paper or fee filed by "Express Mail" *must* have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. 1.10(b).
"Since the filing of correspondence under § 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will *not* be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

                             (Application Transmittal [4-1]—page 1 of 9)

1. Type of Application

This new application is for a(n)

(check one applicable item below)

☒ Original (nonprovisional)

☐ Design

  ☐ Plant

WARNING: Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application.

WARNING: Do not use this transmittal for the filing of a provisional application.

NOTE: If one of the following 3 items apply, then complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED and a NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION.

☐ Divisional.

☐ Continuation.

☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120, or 121)

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c). (35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b).) For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205.

WARNING: When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3).

☐ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

3. Papers Enclosed That Are Required for Filing Date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

_13_ Pages of specification

_3_ Pages of claims

_1_ Pages of Abstract

_3_ Sheets of drawing

☒ formal

☐ informal

(complete the following, if applicable)

☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. 1.84(b).

4. **Additional papers enclosed**

☐ Preliminary Amendment

☐ Information Disclosure Statement (37 C.F.R. 1.98)

☐ Form PTO–1449 (PTO/SB/08A and 08B)

☐ Citations

☐ Declaration of Biological Deposit

☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.

☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative

☐ Special Comments

☐ Other

5. **Declaration or oath**

☒ Enclosed

Executed by

(check all applicable boxes)

☒ inventor(s).

☐ legal representative of inventor(s).
37 CFR 1.42 or 1.43.

☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.

    ☐ This is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. See item 13 below for fee.

☐ Not Enclosed.

☐ Application is made by a person authorized under 37 C.F.R. 1.41(c) on behalf of *all* the above named inventor(s).

(The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently).

NOTE: *It is important that all the correct inventor(s) are named for filing under 37 CFR 1.41(c) and 1.53(b).*

☐ Showing that the filing is authorized.
(not required unless called into question. 37 CFR 1.41(d)}

6. Inventorship Statement

WARNING: *If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.*

The inventorship for all the claims in this application are:

☒ The same.

or

☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,

☐ is submitted.

☐ will be submitted.

7. Language

NOTE: *An application including a signed oath or declaration may be filed in a language other than English. A verified English translation of the non-English language application and the processing fee of $130.00 required by 37 CFR 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 CFR 1.52(d).*

NOTE: *A non-English oath or declaration in the form provided or approved by the PTO need not be translated. 37 CFR 1.69(b).*

☒ English

☐ Non-English

☐ The attached translation is a verified translation. 37 C.F.R. 1.52(d).

8. Assignment

☐ An assignment of the invention to _____

_____

☐ is attached. A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCU-MENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.

☐ will follow.

NOTE: *"If an assignment is submitted with a new application, send two separate letters-one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).*

WARNING: *A newly executed "CERTIFICATE UNDER 37 CFR 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.*

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. No.	Filed

Country	Appln. No.	Filed

Country	Appln. No.	Filed

from which priority is claimed

☐ is (are) attached.

☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 CFR 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. 1.16)

A. ☒ Regular application

CLAIMS AS FILED			
Number filed	Number Extra	Rate	Basic Fee 37 C.F.R. 1.16(a)
		690.00	$790.00
Total Claims (37 CFR 1.16(c)) 17 – 20 = 0	×	$ 22.00	
Independent Claims (37 CFR 1.16(b)) 1 – 3 = 0	×	$ 82.00	
Multiple dependent claim(s), if any (37 CFR 1.16(d))	+	$270.00	

☐ Amendment cancelling extra claims is enclosed.

☐ Amendment deleting multiple-dependencies is enclosed.

☐ Fee for extra claims is not being paid at this time.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 CFR 1.16(d).

Filing Fee Calculation $ 690.00

B. ☐ Design application
(\$330.00—37 CFR 1.16(f))

                   Filing Fee Calculation   \$_____

C. ☐ Plant application
(\$540.00—37 CFR 1.16(g))

                   Filing fee calculation   \$_____

11. Small Entity Statement(s)

     ☐ Verified Statement(s) that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is (are) attached.

WARNING: *"Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. A nonprovisional application may rely on a verified statement filed in the prior application if the nonprovisional application includes a reference to a verified statement in the prior application or includes a copy of the verified statement filed in the prior application if status as a small entity is still proper and desired." 37 C.F.R. § 1.28(a).*

                       (complete the following, if applicable)

     ☐ Status as a small entity was claimed in prior application

         _____ / _____, filed on _____, from which benefit is being claimed for this application under:

         35 U.S.C. ☐ 119(e),
                     ☐ 120,
                     ☐ 121,
                     ☐ 365(c),

         and which status as a small entity is still proper and desired.

         ☐ A copy of the verified statement in the prior application is included.

            Filing Fee Calculation (50% of **A, B or C** above)

                     \$_____

NOTE: Any excess of the full fee paid will be refunded if a verified statement and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendable under § 1.136. 37 CFR 1.28(a).

12. Request for International-Type Search (37 C.F.R. 1.104(d))

                       (complete, if applicable)

     ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☐ Not Enclosed

    ☐ No filing fee is to be paid at this time.
    (This and the surcharge required by 37 C.F.R. 1.16(e) can be paid subse-
    quently.)

☒ Enclosed

    ☒ Filing fee $ ___690.00___

    ☐ Recording assignment
       ($40.00; 37 C.F.R. 1.21(h))
       (See attached "COVER SHEET FOR
       ASSIGNMENT ACCOMPANYING NEW
       APPLICATION".) $ _____

    ☐ Petition fee for filing by other than all the
       inventors or person on behalf of the inventor
       where inventor refused to sign or cannot be
       reached
       ($130.00; 37 C.F.R. 1.47 and 1.17(h)) $ _____

    ☐ For processing an application with a
       specification in
       a non-English language
       ($130.00; 37 C.F.R. 1.52(d) and 1.17(k)) $ _____

    ☐ Processing and retention fee
       ($130.00; 37 C.F.R. 1.53(d) and 1.21(l)) $ _____

    ☐ Fee for international-type search report
       ($40.00; 37 C.F.R. 1.21(e)) $ _____

NOTE: *37 CFR 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing
to complete the application pursuant to 37 CFR 1.53(d) and this, as well as the changes to 37 CFR
1.53 and 1.78, indicate that in order to obtain the benefit of a prior U.S. application, either the basic
filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from
notification under § 53(d).*

                         Total fees enclosed $___690.00___

14. Method of Payment of Fees

☒ Check in the amount of $___690.00___

☐ Charge Account No. _____ in the amount of
    $_____
    A duplicate of this transmittal is attached.

NOTE: *Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 CFR
1.22(b).*

15. Authorization to Charge Additional Fees

WARNING: *If no fees are to be paid on filing, the following items should* not *be completed.*

WARNING: *Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized.*

☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 19-0590 :

  ☒ 37 C.F.R. 1.16(a), (f) or (g) (filing fees)

  ☒ 37 C.F.R. 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: *Because additional fees for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency (37 CFR 1.16(d)), it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.*

  ☐ 37 C.F.R. 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

  ☐ 37 C.F.R. 1.17 (application processing fees)

WARNING: *While 37 CFR 1.17(a), (b), (c) and (d) deal with extensions of time under § 1.136(a), this authorization should be made only with the knowledge that: "Submission of the appropriate extension fee under 37 C.F.R. 1.136(a) is to no avail* unless *a request or petition for extension is filed." (Emphasis added). Notice of November 5, 1985 (1060 O.G. 27).*

  ☐ 37 C.F.R. 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. 1.311(b))

NOTE: *Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 CFR 1.311(b).*

NOTE: *37 CFR 1.28(b) requires "Notification of any change in status resulting in loss of entitlement to small entity status must be filed in the application . . . prior to paying, or at the time of paying, . . . issue fee." From the wording of 37 CFR 1.28(b), (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

16. Instructions as to Overpayment

  ☒ Credit Account No. 19-0590
  ☐ Refund

Reg. No. 24,518

Tel. No. (408) 297-9733

Customer No. 003897

/Thomas Schneck/ (signature)

SIGNATURE OF PRACTITIONER

Thomas Schneck

(type or print name of attorney)

P.O. Box 2-E

P.O. Address

San Jose, CA 95109-0005

☐ **Incorporation by reference of added pages**

> *(check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an international application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED)*

    ☐ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

        Number of pages added _____

    ☐ Plus Added Pages for Papers Referred to in Item 4 Above

        Number of pages added _____

    ☐ Plus "Assignment Cover Letter Accompanying New Application"

        Number of pages added _____

☒ **Statement Where No Further Pages Added**

> *(if no further pages form a part of this Transmittal, then end this Transmittal with this page and check the following item)*

    ☒ This transmittal ends with this page.

Description

SECURE TRANSACTIONS WITH
PASSIVE STORAGE MEDIA

5

TECHNICAL FIELD

The present invention relates to passive data
storage media, such as optical memory cards, and
transaction systems making use of such media, and in
10   particular relates to measures taken to ensure secure
transactions.

BACKGROUND ART

In U.S. Patent No. 5,694,471, Chen et al.
15   disclose a system for preventing fraudulent use of
identity or transaction cards. The cards are chip cards
that include an integrated circuit with a unique serial
number permanently and unalterably burned into the chip,
and having sufficient storage capacity for a card issuer
20   identification (ID) number, user information (name,
account number, signature image, etc.), the public key of
a public-private key pair, a digital signature, and a
personal identification number (PIN) derived from a user
password. To initialize a card, a one-way hash function
25   is performed on the issuer ID and user information to
obtain a checksum, an XOR operation is performed on the
checksum and card serial number to obtain a composite
result, and this result is enciphered using the private
key of the public-private key pair to obtain the digital
30   signature. Also, the PIN is obtained by enciphering the
card serial number using a user-entered password as the
key. In carrying out a transaction at a processing
terminal, a card is authenticated by deciphering its
digital signature using its public key to recover the
35   composite result, performing an XOR operation on the
composite result and card serial number to recover the
checksum, performing a one-way hash function on the
issuer ID and user information to compute a checksum and

comparing the recovered and computed checksums, which
should match if the card is authentic. The user is
authenticated by enciphering the card serial number using
a user-entered password as the key to compute a PIN and
5   then comparing it with the stored PIN on the card to
determine whether they match.

        In U.S. Patent No. 5,999,626, Mullin et al.
disclose a digital signature scheme for a smart card in
which signature components for a transaction session are
10   generated partly by the processing chip on the card and
partly by the associated transaction terminal. In
particular, a signature composed of a pair of elements is
generated for a session by combining another pair of
elements selected from a set of prestored signing
15   elements on the card, with the initial step in the
computation being performed by the processing chip on the
card and the result thereof transferred to the
transaction device for the additional steps in the
derivation. Thus, the identity of the signing elements
20   prestored on the card is not revealed to the transaction
terminal, but the bulk of the computation is implemented
by the terminal instead of by the processing chip on the
card.

        These examples illustrate some of the ways in
25   which secure transactions may be carried out when using a
smart card, which has an embedded microprocessor chip in
it. Thus, a smart card can encrypt and decrypt data (or
share part of the computation with another device), that
is saved internally in its memory.

30   In contrast, passive storage media, such as
optical memory cards (OMCs), memory chip cards, compact
disks (CD-R and CD-RW), or magnetic media, don't have a
microprocessor chip. While they have large memory
capacity useful for storing complete transaction records,
35   they have not been deemed sufficiently secure for
transaction applications like e-commerce. Any
transaction system involving passive media will, like
those involving smart cards, require card and user

authentication protocols, and also will certainly need to
have its stored transaction data be encrypted. Some
computers already have encryption and protocol control
processors inside the hardware, and some IC-chip readers
5   already have some protocol control processors inside
them. But in a system using passive storage media,
software/firmware protocols and encryption of the data
stored on the media will not be enough to ensure adequate
security. Other system security components will be
10 needed to prevent interception of decrypted data at any
weak link in the transaction system and access to the
encryption/decryption keys will need to be denied to all
but authorized persons. To date, such security measures
have been unavailable to systems that use passive storage
15 media and, thus, in comparison to smart cards. The
passive media systems have been deemed too insecure for
those transactions which are vulnerable to fraud or
forgery (e.g., financial transactions).

         It is an object of the present invention to
20 provide data security methods and systems for achieving
secure transactions when using passive storage media,
such as optical memory cards.
         It is another object of the present invention
to provide both hardware and software/firmware security
25 measures to deny unauthorized access to cryptographic
keys and to prevent interception of decrypted data
streams.

DISCLOSURE OF THE INVENTION
30   These objects have been met by a transaction
system that secures the read/write drive for the passive
medium and the drive-host communications link from
unauthorized access to the cryptographic keys and
decrypted transaction data. The drive provides the
35 encryption and decryption processing for the medium
(since the medium lacks an embedded processor chip),
provides authentication of users presenting a passive
medium for a transaction, and is tamper resistant to

thwart attempts to gain access to the cryptographic keys.
Further, the drive's communication link with a host
computer is also conducted using only encrypted data and
secure protocols, so that no decrypted data stream is
5   available for interception at any point in the system and
only authorized communications will be recognized by the
system. Only the host computer can extract or decrypt
messages (commands and data) received from a drive.
          Validation of a user is performed through a
10   combination of a digital signature derived from a user-
entered keyword or personal identification number (PIN)
and digital certificates used by a trusted certificate
authority. Each passive storage medium and each drive
may have several unique keys and certificates, e.g. for
15   different partitions or sections of the medium and for
different operations or types of transactions to be
mediated by the drive.

BRIEF DESCRIPTION OF THE DRAWINGS
20   Fig. 1 is a schematic plan view of a hardware
architecture for a transaction system in accord with the
present invention.
          Fig. 2 is a tree diagram illustrating a digital
certificate hierarchy issuing certificates used by the
25   transaction system of the present invention.
          Fig. 3 is a flow diagram for enrolling a user
of the transaction system.
          Fig. 4 is a flow diagram for verifying the
identity of an enrolled user of the transaction system.
30   Fig. 5 is a flow diagram for changing keys used
by a drive of the transaction system.
          Fig. 6 is a flow diagram for storage of secure
data.

BEST MODE FOR CARRYING OUT THE INVENTION
35   With reference to Fig. 1, a transaction system
of the present invention includes a drive 10 for reading
data from and writing data to a passive storage medium

12, such as a optical memory card, and a host computer 14
in data communication with the drive 10 via a
communications link 36, which may be part of a network.
Optical memory cards are cards, about the size of a

5   credit card (e.g. 54 X 86mm), on which is disposed an
optically readable storage medium 16 storing data. The
data can include analog data (watermarks, holograms,
etc.) or digital data (barcodes, spots 17 formed in
tracks, etc.) or both. These data contain information

10   related both to transaction data (messages) and
information related to the security of the messages (keys
and certificates). Optical memory cards that store
digital data can be read by an optical reader writer
which uses a laser diode, photodetector plus some

15   scanning optics, represented figuratively by the element
18 and light 20. Motors 22 move the card 12 and position
it appropriately relative to the light 20. Such optical
read/write devices for optical memory cards are well
known. The solutions realized by the present invention

20   are applicable not only to optical cards, but also any
other passive storage medium (i.e., a medium lacking an
embedded microprocessor), such as magnetic and optical
disks (CD-ROM, CD-R, CD-RW), magnetic memory storage
devices (computer hard drives) and microprocessor-less

25   IC-chip cards, together with the corresponding drives
that drive them.

         The driver 10 further includes a microprocessor
24, some nonvolatile memory 26 (ROM, EPROM, EEPROM), some
volatile memory 28 (RAM) and an I/O interface 34 (such as

30   SCSI) through which the drive 10 is connected to the host
computer 14. In a typical read/write drive for an
optical memory card the microprocessor 24 sends and
receives commands to and from the host computer 14. The
microprocessor 24's firmware is stored on the nonvolatile

35   memory 26. The firmware is code that allows the
microprocessor to interpret the commands and to direct
the modulation of the laser optics 18 to read or write
appropriate information on the card 12. These drive

DTC21:99-09.APL

elements 24-34 are common to both insecure passive media
drives and the secure drives 10 of the present invention.
The secure drives have additional security features,
including a cryptographic processor 30 and sensors 32
5   that protect the drive 10 against intruders. The key or
keys that the drive uses encrypt or decrypt security
information on the optical memory card 12 (secret keys,
digital signatures, etc.), and to encrypt or decrypt
transaction data (messages, commands), are stored in the
10   drive's EEPROM or other non-volatile memory 26. The
drive 10 is made tamper-resistant by taking physical
measures which are known in the art to seal the drive and
thwart attempts to open the drive or otherwise gain
unauthorized access to the keys and other critical
15   information. In particular, the drive 10 is shielded
from attacks that use electromagnetic radiation to peek
inside the unit, e.g. with x-rays, or that monitor signal
radiation emitted by drive circuitry which might
otherwise leak out of the drive. The security sensors 32
20   detect attempts to open the unit, e.g. by cutting. If
such an attack is detected, the unit 10 will erase the
contents of its firmware and all critical information
contained within its memory 26 or 29. It may also
destroy parts of the circuitry by burning some of the
25   components, e.g. cryptographic processor 30. A battery
(not shown) keeps the sensors 32 and critical information
operational in the absence of electricity and is used for
data and component destruction in the event of an attack.
Other physical security measures are also possible.
30   The cryptographic processor 30, in addition to
encrypting and decrypting data written to or read from
the card 12, also provides validation of authorized users
by means of digital signature and certificate protocols,
and further provides encrypting and decrypting of
35   transaction data flowing between the drive 10 and the
host computer 14 over signal lines 36. This scheme turns

the passive storage medium 12 and drive 10 into a "virtual" smart card system, as seen by the host computer 14.

5   With reference to Fig. 2, digital certificates are documents issued in a standard format (e.g., ITU-T x.509) by a certifying authority (CA) attesting that a specific public key belongs to a particular individual or entity. Such certificates typically contain the authorized user's name and other identifying information,

10   together with an associated public key, an expiration date, and the name and digital signature of the issuing certifying authority (CA). Thus, digital certificates are a form of digital signature of the certifying authority using its public key that certify public keys

15   from forgery, false representation or alteration, allowing a receiver of a message (e.g. a transaction instruction or record) to authenticate the message's signature. There may be two or more certificates authenticate a message, forming a hierarchical chain of

20   certificates, in which the authenticity of one certificate is attested by another issued by a higher certifying authority. At the top of the certificate hierarchy is a top-level or "root" certifying authority (CA-0) (e.g., a government agency) and whose public key

25   is widely published so as to be independently known. The issuer of the optical memory card or like passive storage medium, for example, a bank or other financial institution, an insurance company, an HMO or other health provider, an employer, university or municipality is

30   typically a level two or three certifying authority (CA-2 or CA-3). Thus, the root CA-0 entity vouches for high-level CA-1 entities, which in turn vouch for the card issuing CA-2 entities or for CA-2 entities that vouch for card issuing CA-3 entities. Different certifying

35   authorities can have access to different drive operations, including the ability to securely modify protocols and keys embedded in the drive. Different certifying authorities could also have access to

different sections or partitions of a storage medium.
The most certifying authority CA-0 can give certifying
authority to the drives. That is, the certifying
authority (CA) certifies the drive, and the drive

5 certifies other processes, including the drive-computer
and drive-media communications, using its own
certificates. Each drive can issue different types of
certificates, depending on the function at the time.
Each drive is capable of certifying the data before it is

10 stored on the passive medium, and likewise before it is
forwarded to the computer. Because the process of
certification requires digital signatures, encryption and
the like in accord with selected secure protocols, these
capabilities of the drive give the data stored in passive

15 media enhanced security.
          With reference to Fig. 3, optical memory cards
or other passive storage media are issued by an enrollment
process that establishes a user's digital signature for
that medium. While a CA might issue certificates to

20 unaffiliated individuals with proper identification, in a
typical transaction system in accord with the present
invention the card issuing CA would normally issue
transaction cards containing such certificates only to
their members. Thus, a company would issue cards to its

25 own employees, a university to its faculty and students,
an HMO to its doctors and member patients, a bank to its
account holders, etc. In a first enrollment step 41, the
new user produces a message M_1 containing personal data
required by the issuer and selects a password or personal

30 identification number (PIN). The password or PIN is used
by the computer to generate cryptographic keys such as an
asymmetric (private-public)key pair (A_k, a_k). The card could
be issued over a less secure pathway, e.g. remotely over
the Internet, by adding certain additional encryption and

35 certification steps according to a secure protocol, such
as secure sockets layer (SSL), Hands Like Protocol,
developed by Netscape Communications Corp. Even more
commonly, secure protocols are always used regardless of

the supposed security of the communication pathway. Any protocol can be used, including the well established SSL protocol. The new user signs the message M_1 with a private key A_k, and the signed message $A_k(M_1)$ is encrypted by a host

5 computer (step 45) with one of the drive's public keys 61 and the user's public key a_k is attached to obtain an envelope $[E_{b1}(A_k(M_1)),a_k]$ that is sent to the certifying authority issuing the card. The key b1 used to form the envelope is a public key of a tamper-resistant drive

10 associated with the issuer. Such drives store corresponding private keys (B1, etc.) which are inaccessible to the user or any unauthorized person. Private keys generated by the drive can be changed only b1 certain authorized parties, e.g. the card issuer or

15 perhaps only to higher certifying authorities (CA-0 or CA-1). The certifying authority signs the envelope with its private key, $E_{CA}[E_{b1}CA_k(M_1),a_k]$ and sends it to the drive (step 47). The issuer's drive then opens the envelope with the certifying authority's public key,

20 $D_{ca}(E_{CA}[E_{b1}(A_k(M_1)),a_k]) = [E_{b1}(A_k(M_1)),a_k]$, (step 49) to extract the public key a_k. The drive accepts this key as valid because it has been certified. The drive then decrypts the signed message $D_{B1}(E_{b1}(A_k(M_1))) = A_k(M_1)$, using one of its private keys B1 (step 51). At this point, the user's

25 public key a_k could be used to extract the required personal information $D_{ak}(A_k(M_1)) = M_1$.) The card issuer drive next encrypts (step 53) the envelope received from the user using another of its public keys b2 and writes the encrypted envelope $[E_{b2}(A_k(M_1)),a_k]$ to a passive storage

30 medium. Such as an optical memory card. The user is now enrolled for subsequent transactions involving the issuer's drives.

　　　　With reference to Fig. 4, in conducting a transaction, an enrolled user presenting a transaction

35 card must verify his identity. The user inserts the card or other passive medium into a drive (step 61), and enters a password or PIN and a "request verification" command message M_2 (step 63). Again, the password or PIN is used

by a cryptographic processor to derive an asymmetric
(private-public) key pair A_k, a_k. If the user has entered
the correct password or PIN then these keys will match
those used in creating the envelope stored on the card.

5 The command message M_2 is signed (step 65) with the private
key A_k in the derived pair to create the signed message
$A_k(M_2)$.

The user then encrypts (step 67) the signed
message with the transaction terminal's public key b1 and
10 sends the encrypted message $E_{b1}(A_k(M_2))$ over a
communications pathway to the transaction terminal, which
then decrypts (step 69) the received message using a
corresponding private key B1 to obtain the signed message,
$D_{B1}(E_{b1}(A_k(M_2))) = A_k(M_2)$. Next, the transaction terminal
15 reads (step 71) the personal information that was stored
as an envelope on the card during enrollment,
$E_{b2}(A_k(M_1), a_k)$. As this signature is already encrypted,
further encryption is not needed to transmit the
information to the transaction terminal, even if the
20 communications pathway is considered otherwise insecure.
The transaction terminal or drive uses its private key B2
to decrypt (step 73) the signature and obtain the user's
public key a_k, i.e. $D_{B2}(E_{b2}(A_k(M_1), a_k)) = A_k(M_1), a_k$. This
decryption will be successful only if the envelope from
25 the storage medium is valid, such that the terminal drive
has a private key B2 corresponding to the public key b2
used to create the envelope during enrollment. The
transaction terminal then uses this user public key a_k
obtained from the card to decrypt (step 75) the signed
30 message, $D_{ak}(A_k(M_2)) = M_2$. When the public key obtained
from the decrypted envelope read from the card corresponds
to the private key derived from the user-entered PIN that
was used to sign the message M_2, the decryption will be
successful and the transaction terminal will be assured
35 that the user is valid. The transaction terminal fulfills
the user's request command by then decrypting (step 77)
the user's original message, M_1, stored in the digital
signature on the card, $D_{ak}(A_k(M_1)) = M_1$, thereby revealing

the user account information that enables a transaction to
be conducted. The transaction terminal transmits this
information to the host computer for validation of the
transaction request by first encrypting (step 79) an
5   envelope containing the signed message $A_k(M_1)$ and public
key a_k from its with one of its private keys B1. The
encrypted message $E_{B1}(A_k(M_1),a_k)$ is decrypted (step 81) by
the user with the corresponding public key of the
transaction terminal, $D_{b1}(E_{B1}(A_k(M_1),a_k)) = A_k(M_1),a_k$, when
10   then validates the transaction request.

            The encryption, digital signatures, certificates
of any data by the host (computer, network, etc.) allows
only a secure transmission to the drive, and vice versa
when the drive encrypts and signs any data. That data is
15   then re-encrypted with a combination of original keys and
unique (new) keys generated by and inside the drive before
they are stored on the media. In other words, the
encrypted data, digitally signed and certified, does not
externally resemble the same data as it was sent by a
20   computer to the drive. The fundamental reasons for those
separate processes are (a) to prevent any monitoring of
communications between computer and drive from shedding
any light on what is being stored on the media, (b) to
establish, by a kind of "remapping", a relationship
25   between the drive and media that is unique and different
from the relationship between the host computer and the
drive, and (c) to prevent anyone trying to make an exact
bit copy of the media from knowing what data is being
stored and how that data is being stored.

30   Occasionally, there will be a need to either
add, delete or change keys inside the drive. Protocols
could also be changed. The root authority CA-0 or a top-
level authority CA-1 higher than the issuing authority CA-
2 or CA-3 associated with the particular drive can certify
35   the new keys. With reference to Fig. 5, a message M_3
containing the new keys (starting point 91 in Fig. 5) and
commands directing the change or addition of keys, is
signed by the certifying authority (CA), as seen in step

93, $CA_k(M_3)$. This is done using CA's private key CA_k. The CA creates a digital envelope (step 95), encrypting the signed message with a public key of the drive whose key's are being changed or added to and sends the envelope,

5      $E_{B1}(CA_k(M_3))$ to that drive. The drive decrypts (step 97) the envelope, $D_{b1}(E_{B1}(CA_k(M_3))) = CA_k(M_3)$, and then decrypts (step 99) the signed message with the CA's public key ca_k, $D_{cak}(CA_k(M_3)) = M_3$. The certified new keys are added (or replace some or all, old keys) in the drive's secure

10   EEPROM (step 101).

       With reference to Fig. 6, if a user wants to store very sensitive information on the passive storage medium, such as transaction account information relating to the user, so that it will be accepted as valid on

15   feature reads by a drive or host computer, then it meets not only to be encrypted but also certified. The data is in the form of a message M_4, which is encrypted (step 111) by the user with a symmetric key S_A to produce the envelope $S_A(M_4)$. A certifying authority then signs the envelope

20   (step 113) the envelope with the certifying authority's public key, $D_{cak}(E_{CAk}[S_A(M_4)]) = S_A(M_4)$, and then encrypts (step 117) the user's signed message with another of its private keys, $E_{B2}(S_A(M_4))$ and unites it (step 119) to the storage medium.

25   These examples of preferred digital signature protocols using digital certificates show how a passive storage medium can be used in secure transactions when used with tamper resistant drives containing cryptographic processors. Other protocols, such as SSL, could be used

30   as well. The media store encrypted transaction data and a encrypted digital certificate containing a user encrypted digital signature. Access to drive encryption keys are restricted, while allowing drive operation by authorized persons presenting a valid storage medium with a user

35   keyword or PIN. The digital certificate must be renewed periodically, as it contains an expiration date as part of the message or envelope. (Certificates might also be revised prior to their scheduled expiration date by using

protocols involving certificate revokation lists (CRLs)
listing current certificates.) Transaction data
communication between the drive and a host computer is
also encrypted using either public key or, preferably,
5   secret key (symmetric) encryption so that there are no
weak links in the system through which transaction or
encryption key data might otherwise become open to
unauthorized inspection. Hence, secure transactions with
passive media are now possible.

Claims

1. A secure transaction system, comprising:

a plurality of information carriers distributed to authorized users for secure storage of information related to carrying out of transactions by said authorized users, each information carrier having a passive data storage medium but lacking any data processing unit, said information stored on said medium being in encrypted form and including transaction messages, crytographic keys, digital signatures and at least one digital certificate issued to an authorized user;

a tamper-resistant drive for reading and writing information relating to transactions on an information carrier presented thereto by an authorized user, said drive connected via a communications link or network to a host computer, said drive having a control unit executing secure protocols for mediating communication between said host computer and drive and between said drive and information carrier, said drive also having a cryptographic processing unit providing encryption and decryption of transaction messages and digital certificates in accord with said secure protocols executed by said control unit and using cryptographic keys, including keys stored by said drive and keys read from said information carriers, as specified by said secure protocols.

2. The system of claim 1 wherein said data processing unit of said drive also providing, as specified by said secure protocols, encryption and decryption of information communicated with said host computer via said communications link.

3. The system of claim 1 wherein said drive includes
sensors detecting attempted intrusions into the drive,
said control unit being responsive to said sensors for
destroying critical cryptographic keys in the drive upon
detection of any intrusion.

4. The system of claim 1 wherein said storage medium on
said information carrier comprises optical media.

5. The system of claim 4 wherein said information
carrier is on optical memory card.

6. The system of claim 4 wherein said information
carrier is an optical disk.

7. The system of claim 4 wherein information is stored
on said storage medium in accord with a specified format.

8. The system of claim 1 wherein said information stored
on said information carrier is in encrypted form
corresponding to a decryption key stored in said tamper-
resistant drive.

9. The system of claim 8 wherein said information stored
on said information carrier also includes personal data
for generating keys of said authorized user.

10. The system of claim 9 wherein said personal data
comprises any of a personal identification number (PIN),
a password, and biometric data.

11. The system of claim 1 wherein said storage medium is logically partitioned and at least one different digital certificate is stored thereon for each partition.

12. The system of claim 1 wherein said secure protocols include an enrollment of an authorized user wherein personal data for said user is digitally signed, and transmitted from a host computer to said drive with at least one digital certificate, and recertified by said drive and stored on said passive storage medium.

13. The system of claim 1 wherein said secure protocols include a transaction by an authorized user wherein transaction requests and authorization information and transmitted between said drive and said host computer and between said drive and said storage medium with at least one digital certificate.

14. The system of claim 1 wherein said secure protocols executed by said drive include at least one protocol that permits modification of said keys stored by said drive.
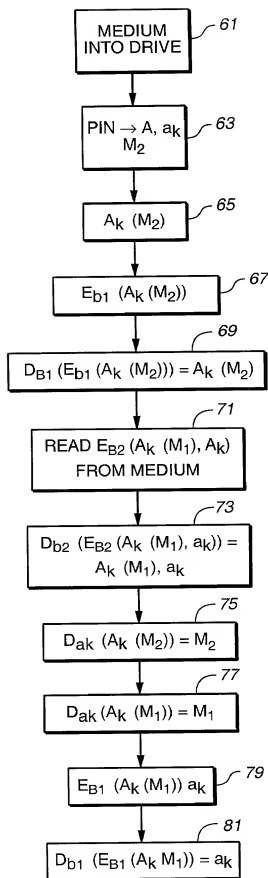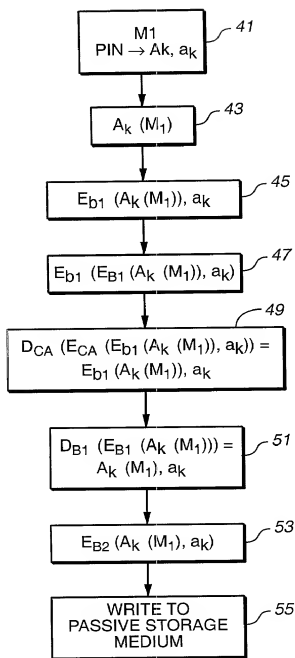
15. The system of claim 14 wherein said protocol permitting modification of said keys is one of said protocols mediating communications between said host computer and said drive.

16. The system of claim 14 wherein said protocol permitting modification of said keys is one of said protocols mediating communication between said drive and said information carriers.
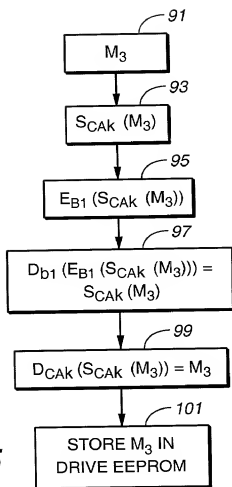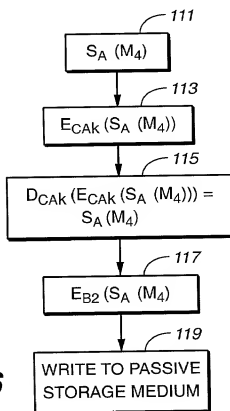
17. The system of claim 14 wherein at least one of said secure protocols also permits modification of the secure protocols themselves.

Abstract of the Disclosure

A transaction system for use with passive data storage media, such as optical memory cards, uses secure
5   protocols involving digital certificates for communication between a read/write drive and the medium and also for communication between the drive and a host computer. The drive is physically secured with tamper resistant features and stores cryptographic keys and
10   firmware for executing the secure protocols. All messages (data or commands) passed between the drive and the passive medium or host computer not only are encrypted but also include at least one digital certificate for authenticating the message. Typically,
15   asymmetric (public-private key) encryption is used and keys may be derived from an authorized user's password, personal identification number, or biometric data. The drive includes sensors to detect any attempted intrusions and a control unit that will destroy the critical
20   information (keys and protocol code) in response to a detected intrusion. The keys and protocols stored in a drive can themselves be changed through appropriate use of a secure protocol involving digital certificates.

FIG._1

FIG._2

FIG._3

- $M1$ $PIN \rightarrow A_k, a_k$ — 41
- $A_k (M_1)$ — 43
- $E_{b1} (A_k (M_1)), a_k$ — 45
- $E_{b1} (E_{B1} (A_k (M_1)), a_k)$ — 47
- $D_{CA} (E_{CA} (E_{b1} (A_k (M_1)), a_k)) = E_{b1} (A_k (M_1)), a_k$ — 49
- $D_{B1} (E_{B1} (A_k (M_1))) = A_k (M_1), a_k$ — 51
- $E_{B2} (A_k (M_1), a_k)$ — 53
- WRITE TO PASSIVE STORAGE MEDIUM — 55

FIG._4

- MEDIUM INTO DRIVE — 61
- $PIN \rightarrow A, a_k$ M_2 — 63
- $A_k (M_2)$ — 65
- $E_{b1} (A_k (M_2))$ — 67
- $D_{B1} (E_{b1} (A_k (M_2))) = A_k (M_2)$ — 69
- READ $E_{B2} (A_k (M_1), A_k)$ FROM MEDIUM — 71
- $D_{b2} (E_{B2} (A_k (M_1), a_k)) = A_k (M_1), a_k$ — 73
- $D_{ak} (A_k (M_2)) = M_2$ — 75
- $D_{ak} (A_k (M_1)) = M_1$ — 77
- $E_{B1} (A_k (M_1)) a_k$ — 79
- $D_{b1} (E_{B1} (A_k M_1)) = a_k$ — 81

$$M_3 \quad \text{— } 91$$

$$S_{CAk}(M_3) \quad \text{— } 93$$

$$E_{B1}(S_{CAk}(M_3)) \quad \text{— } 95$$

$$D_{b1}(E_{B1}(S_{CAk}(M_3))) = S_{CAk}(M_3) \quad \text{— } 97$$

$$D_{CAk}(S_{CAk}(M_3)) = M_3 \quad \text{— } 99$$

STORE M_3 IN DRIVE EEPROM — 101

FIG._5

$$S_A(M_4) \quad \text{— } 111$$

$$E_{CAk}(S_A(M_4)) \quad \text{— } 113$$

$$D_{CAk}(E_{CAk}(S_A(M_4))) = S_A(M_4) \quad \text{— } 115$$

$$E_{B2}(S_A(M_4)) \quad \text{— } 117$$

WRITE TO PASSIVE STORAGE MEDIUM — 119

FIG._6

07-10-00

A

Please type a plus sign (+) inside this box → +

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)		
	Attorney Docket Number	DTC 99-09
	First Named Inventor	Louis H. Sciupac
	COMPLETE IF KNOWN	
	Application Number	/
	Filing Date	
☒ Declaration Submitted with Initial Filing OR ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)	Group Art Unit	
	Examiner Name	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

> SECURE TRANSACTIONS WITH PASSIVE STORAGE MEDIA

the specification of which   *(Title of the Invention)*
☒ is attached hereto
   OR
☐ was filed on (MM/DD/YYYY) [   ]   as United States Application Number or PCT International

Application Number [   ]   and was amended on (MM/DD/YYYY) [   ]   (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	
		☐ Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Please type a plus sign (+) inside this box → [+]

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT International application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: ☒ Customer Number [003897] → Place Customer Number Bar Code Label here
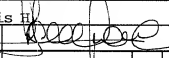OR
☒ Registered practitioner(s) name/registration number listed below

Name	Registration Number	Name	Registration Number
Thomas Schneck	24,518	David M. Schneck	43,094
Mark Protsik	31,788	Rosalio Haro	42,633
John P. McGuire	41,984	Gina McCarthy	42,986

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☒ Customer Number [003897] or Bar Code Label   OR ☒ Correspondence address below

Name	Thomas Schneck
Address	P.O. Box 2-E
Address	
City	San Jose	State	CA	ZIP	95109-0005
Country	U.S.A.	Telephone	(408) 297-9733	Fax	(408) 297-9748

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle, if any)	Family Name or Surname
Louis H.	Sciupac

Inventor's Signature		Date	7/6/2000

Residence: City	Santa Clara	State	CA	Country	U.S.A.	Citizenship	U.S.A.

Post Office Address	528 Hubbard Avenue
Post Office Address	
City	Santa Clara	State	CA	ZIP	95051	Country	U.S.A.

☐ Additional inventors are being named on the ___ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto